

UNEXTENDIBLE MUTUALLY UNBIASED BASES (AFTER MANDAYAM, BANDYOPADHYAY, GRASSL AND WOOTTERS)

KOEN THAS

ABSTRACT. We consider questions posed in a recent paper of Mandayam, Bandyopadhyay, Grassl and Wootters [10] on the nature of “unextendible mutually unbiased bases.” We describe a conceptual framework to study these questions, using a connection proved by the author in [19] between the set of nonidentity generalized Pauli operators on the Hilbert space of N d -level quantum systems, d a prime, and the geometry of non-degenerate alternating bilinear forms of rank N over finite fields \mathbb{F}_d . We then supply alternative and short proofs of results obtained in [10], as well as new general bounds for the problems considered in *loc. cit.* In this setting, we also solve Conjecture 1 of [10], and speculate on variations of this conjecture.

PACs numbers: 02.10.Hh, 02.40.Dr, 03.67.-a, 03.65.Ta, 03.65.Ud

CONTENTS

| | |
|---|----|
| 1. Introduction | 1 |
| 2. The general Pauli group | 2 |
| 3. Unextendible sets of MUBs and operator classes | 3 |
| 4. Symplectic polar spaces and the Pauli group | 4 |
| 5. Unextendable mutually unbiased bases and Pauli classes | 4 |
| 6. The case d prime, $N = 2$ — small and large examples | 5 |
| 7. Solution of Conjecture 1.2 | 8 |
| 8. Existence of maximal Pauli classes | 9 |
| 9. “Galois MUBs” | 11 |
| 10. Conclusion | 13 |
| Appendix A. Properties of (symplectic) polar spaces | 14 |
| Appendix B. Some more properties of $\mathcal{W}_3(d)$ | 15 |
| References | 16 |

1. INTRODUCTION

Finite-dimensional quantum systems — that is, “multiple qudits” — exhibit many interesting properties like quantum entanglement and quantum non-locality and play, therefore, a crucial role in numerous physical applications like Quantum Cryptography, Quantum Coding, Quantum Cloning/Teleportation and/or Quantum Computing, to mention just a few. As these systems live in finite-dimensional Hilbert spaces, further insights into their behavior require, obviously, a proper understanding of the structure of the associated Hilbert spaces. Within the past few years, a lot of activity in this direction has been devoted to the study of so-called mutually unbiased bases (“MUBs”).

Recall that two orthonormal bases \mathcal{B} and \mathcal{B}' of the Hilbert space \mathbb{C}^ℓ ($\ell \in \mathbb{N}^\times$) are *mutually unbiased* if and only if

$$|\langle \phi | \psi \rangle|^2 = 1/\ell$$

for all $|\phi\rangle \in \mathcal{B}$ and $|\psi\rangle \in \mathcal{B}'$. It is a fundamental conjecture, with many applications, that the theoretical upper bound $\ell + 1$ of a set of mutually unbiased bases can only be reached when ℓ is a *prime power*.

It has been suspected for a long time that there are deep connections between Quantum (Information) Theory and Finite Geometry — see, for instance, Wootters [22, 23]. (See also [5]–[6] and [14]–[16], and references therein.)

As a specific example, proving a conjecture of Saniga and Planat [16], the author showed in [19] that the generalized Pauli operators can be identified with the points, and maximum sets of pairwise commuting members of them with the lines (or subspaces of higher dimensions), of a specific finite incidence geometry so that the structure of the operator space can fully be inferred from the properties of the geometry in question. The incidence geometry is the geometry of a non-degenerate alternating bilinear form over a finite field, called *symplectic polar space*. Using this connection, it is easy to construct maximal sets of MUBs by just translating known results in the theory of symplectic polar spaces.

In a recent paper [10], Mandayam, Bandyopadhyay, Grassl and Wootters introduced *unextendible mutually unbiased bases* (“UMUBs”) (and several variations and related concepts; details can be found in §3) as a natural generalization of maximal sets of mutually unbiased bases.

One of the main results of [10] reads as follows.

Theorem 1.1 (Mandayam et al. [10]). *Given three Pauli classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ belonging to a complete set \mathcal{S} of classes in $d = 4$, there exists exactly one more maximal commuting class \mathcal{C} of Pauli operators in $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$. The class \mathcal{C} together with the remaining two classes \mathcal{C}_4 and \mathcal{C}_5 of \mathcal{S} forms an unextendible set of Pauli classes, whose common eigenbases form a weakly UMUB of order 3.*

Using the connection with the polar space, we will give a short proof of this result. Moreover, we generalize this result for all dimensions $\ell = \text{prime}^2$. (In fact, we present a construction of a new class of maximal partial spreads of the symplectic polar space $\mathcal{W}_3(\ell)$ for any odd prime power ℓ , which translates to UMUBs in the case ℓ is a prime.) In dimension $\ell = 8$, a similar result is obtained in [10].

Motivated by Theorem 1.1 and the result in dimension 8, the following conjecture is then stated in [10].

CONJECTURE 1.2 (Mandayam et al. [10]). *Given $\ell/2 + 1$ maximal commuting Pauli classes $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{\ell/2+1}$ belonging to a complete set \mathcal{S} of classes in $\ell = 2^n =: d^n$, there exists exactly one more maximal commuting class \mathcal{C} of Pauli operators in $\cup_{1 \leq i \leq \ell/2+1} \mathcal{C}_i$. The class \mathcal{C} together with the remaining classes of \mathcal{S} forms an unextendible set of Pauli classes of size $\ell/2 + 1$, whose common eigenbases form a weakly UMUB of order $\ell/2 + 1$.*

We will show that this conjecture is true *if and only if* $n = 2$ or $n = 8$. In fact, we will consider the conjecture in any characteristic d (i.e., for any prime d), and show that it is true if and only if $d = 2$ and $n = 2$ or $n = 8$.

We then indicate that an alternative version of the conjecture might be true, and describe several new construction techniques to obtain weakly unextendible sets of MUBs.

At the end of the paper, we discuss a special kind of weakly unextendible sets of MUBs, called “Galois MUBs,” which attain an optimal bound in relation to being unextendible.

Acknowledgement. The author wishes to thank Marcus Grassl and William K. Wootters for various interesting communications on the subject of this note.

2. THE GENERAL PAULI GROUP

Let d be an odd prime. Let $\{|s\rangle | s = 0, 1, \dots, d-1\}$ be a computational base of \mathbb{C}^d . Define the d^2 (generalized) Pauli operators of \mathbb{C}^d as

$$(X_d)^a (Z_d)^b, \quad a, b \in \{0, 1, \dots, d-1\},$$

where X_d and Z_d are defined by the following actions

$$X_d|s\rangle = |s+1 \bmod d\rangle, \quad Z_d|s\rangle = \omega^s|s\rangle,$$

where $\omega = \exp(2i\pi/d)$.

The set \mathbb{P} of generalized Pauli operators of the N -qudit Hilbert space \mathbb{C}^{d^N} is the set \mathbb{P} of d^{2N} distinct tensor products of the form

$$\sigma_{i_1} \otimes \sigma_{i_2} \otimes \cdots \otimes \sigma_{i_N},$$

where the σ_{i_k} run over the set of (generalized) Pauli matrices of \mathbb{C}^d . Denote $\mathbb{P}^\times = \mathbb{P} \setminus \{\mathbf{I}\}$. These operators generate a group $\mathbf{P} = \mathbf{P}_N(d)$ — the *general Pauli group* or *discrete Heisenberg-Weyl group* — under ordinary matrix multiplication, which has order d^{2N+1} .

For the case of N -qubit Hilbert spaces, we refer the reader to [19] — it is completely similar.

3. UNEXTENDIBLE SETS OF MUBS AND OPERATOR CLASSES

Let \mathcal{U} be a set of d^2 mutually orthogonal unitary operators in \mathbb{C}^d using the Hilbert-Schmidt norm: operators A and B are *orthogonal* if $\text{tr}(AB^\dagger) = 0$. Along with the identity operator \mathbf{I} , \mathcal{U} constitutes a basis for the \mathbb{C} -vector space of $(d \times d)$ -complex matrices $\mathbf{M}_{d \times d}(\mathbb{C})$. A standard construction of MUBs outlined in [1] relies on finding classes of commuting operators, with each class containing $d-1$ mutually orthogonal commuting unitary matrices different from the identity \mathbf{I} .

3.1. Maximal commuting operator classes. A set of subsets $\{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_\ell | \mathcal{C}_j \subset \mathcal{U} \setminus \{\mathbf{I}\}\}$ of size $|\mathcal{C}_j| = d-1$ constitutes a (partial) partitioning of $\mathcal{U} \setminus \{\mathbf{I}\}$ into *mutually disjoint maximal commuting classes* if the subsets \mathcal{C}_j are such that

- (a) the elements of \mathcal{C}_j commute for all $1 \leq j \leq \ell$ and
- (b) $\mathcal{C}_j \cap \mathcal{C}_k = \emptyset$ for all $j \neq k$.

In the rest of the paper, we use the term “Pauli classes” to refer to mutually disjoint maximal commuting classes formed out of the N -qudit Pauli group $\mathbf{P}_N(d) \leq \mathbf{U}_{d^N}(\mathbb{C})$.¹ The correspondence between maximal commuting operator classes and MUBs is stated in the following lemma, originally proved in [1].

Lemma 3.1 ([1]). *The common eigenbases of ℓ mutually disjoint maximal commuting operator classes form a set of ℓ mutually unbiased bases.*

3.2. Unextendibility of MUBs and operator classes. A set of MUBs $\{B_1, B_2, \dots, B_\ell\}$ is called *unextendible* if there does not exist another basis that is unbiased with respect to the bases B_1, \dots, B_ℓ .

The correspondence between MUBs and maximal commuting operator classes gives rise to a weaker notion of unextendibility, based on unextendible sets of such classes.

DEFINITION 3.2 (Unextendible sets of operator classes [10]). A set of mutually disjoint maximal commuting classes $\{\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_\ell\}$ of operators drawn from a unitary basis \mathcal{U} is said to be *unextendible* if no other maximal class can be formed out of the remaining operators in $\mathcal{U} \setminus (\{\mathbf{I}\} \cup \bigcup_{i=1}^\ell \mathcal{C}_i)$.

The eigenbases of such an unextendible set of classes form a weakly unextendible set of MUBs, as defined below.

DEFINITION 3.3 (Weakly unextendible sets of MUBs [10]). Given a set of MUBs $\{B_1, B_2, \dots, B_\ell\}$ that are realized as common eigenbases of a set of ℓ operator classes comprising operators from \mathcal{U} , the set $\{B_1, B_2, \dots, B_\ell\}$ is *weakly unextendible* if there does not exist another unbiased basis that can be realized as the common eigenbasis of a maximal commuting class of operators in \mathcal{U} .

¹In [10], only qubits are considered.

4. SYMPLECTIC POLAR SPACES AND THE PAULI GROUP

Consider the projective space $\mathbf{PG}(2N-1, d)$ of dimension $2N-1$, $N \geq 2$, over the field \mathbb{F}_d with d elements, d an odd prime. Let F be a non-degenerate symplectic form of $\mathbf{PG}(2N-1, d)$. For F one can choose the following canonical bilinear form [7]:

$$(X_0Y_1 - X_1Y_0) + (X_2Y_3 - X_3Y_2) + \cdots + (X_{2N-2}Y_{2N-1} - X_{2N-1}Y_{2N-2}).$$

Then the *symplectic polar space* $\mathcal{W}_{2N-1}(d)$ consists of the points of $\mathbf{PG}(2N-1, d)$ together with all totally isotropic spaces of F [7]. Here, a *totally isotropic subspace* is a linear subspace of $\mathbf{PG}(2N-1, d)$ that vanishes under F .

One can also define this space in the underlying $2N$ -dimensional vector space $V(2N, d)$ over \mathbb{F}_d using a non-degenerate alternating bilinear form (which induces a symplectic form on the projective space).

Remark 4.1 (Number of points). Note that $|\text{points of } \mathcal{W}_{2N-1}(d)| = \frac{|V(2N, d)|-1}{d-1} = d^{2N-1} + d^{2N-2} + \cdots + 1$.

In the following proposition, $[\cdot, \cdot]$ denotes the commutator relation in the group \mathbf{P} .

Proposition 4.2 (K. Thas [19]). (i) *The derived group $\mathbf{P}' = [\mathbf{P}, \mathbf{P}]$ equals the center $Z(\mathbf{P})$ of \mathbf{P} .*

(ii) *We have $Z(\mathbf{P}) = \langle \omega \mathbf{I} \rangle$, so that $|Z(\mathbf{P})| = d$.*

(iii) *\mathbf{P} is nonabelian of exponent d .*

(iv) *We have the following short exact sequence of groups:*

$$1 \mapsto Z(\mathbf{P}) \mapsto \mathbf{P} \mapsto V(2N, d) \mapsto 1.$$

Remark 4.3. Note that if $d = 2$, \mathbf{P} is nonabelian of exponent 4.

Now denote the natural map $\mathbf{P} \mapsto V(2N, d)$ by an overbar. Then the commutator

$$[\cdot, \cdot] : V(2N, d) \times V(2N, d) \mapsto \langle \omega \mathbb{I}_{dN} \rangle : (\overline{v_1}, \overline{v_2}) \mapsto [\overline{v_1}, \overline{v_2}] = [v_1, v_2]$$

defines a non-degenerate alternating bilinear form on $V(2N, d)$, so defines a symplectic polar space $\mathcal{W}_{2N-1}(d)$. Here the derived group \mathbf{P}' is identified with the additive group of \mathbb{F}_d .

Theorem 4.4 ([19]). *Two elements of \mathbb{P}^\times commute if and only if the corresponding points of $\mathcal{W}_{2N-1}(d)$ are collinear. In other words, the commuting structure of \mathbf{P} (and \mathbb{P}) is governed by that of the symplectic polar space $\mathcal{W}_{2N-1}(d)$.*

Applying this result, one can easily construct sets of MUBs of maximal size $\ell + 1$ using the symplectic geometry [19].

5. UNEXTENDABLE MUTUALLY UNBIASED BASES AND PAULI CLASSES

In this section, we explain in detail the correspondence between Pauli classes and generators of symplectic polar spaces of [19]. It has the same proof as Theorem 4.4, but we make the relation between (unextendable) commuting Pauli classes and the generators more explicit.

Theorem 5.1 (General connecting theorem). *Two elements of \mathbb{P}^\times commute if and only if the corresponding points of $\mathcal{W}_{2N-1}(d)$ are collinear. In other words, the commuting structure of \mathbf{P} (and \mathbb{P}) is governed by that of the symplectic polar space $\mathcal{W}_{2N-1}(d)$. As a corollary, “complete” partial spreads of $\mathcal{W}_{2N-1}(d)$, correspond to unextendable sets of operator classes in the Pauli group.*

We indicate the proof in several steps.

Let d be any prime and $N \in \mathbb{N} \setminus \{0, 1\}$. Let \mathcal{S} be a *partial spread* of $\mathcal{W}_{2N-1}(d)$, i.e., a set of $(N-1)$ -dimensional isotropic subspaces which are two by two disjoint. Let $M+1$ be the number of elements in \mathcal{S} , and note that $M+1 \leq d^N + 1$ (equality holds when \mathcal{S} is a spread). Then \mathcal{S} corresponds to a set of mutually unbiased bases in the associated d^N -dimensional Hilbert space, in the following way.

- Step 1 To \mathcal{S} corresponds a set of $M+1$ subgroups $H_i, i \in \{0, 1, \dots, M\}$, of \mathbf{P} of size d^{N+1} which mutually (two by two) intersect (precisely) in $Z(\mathbf{P})$.
- Step 2 In each H_j one chooses $d^N - 1$ elements $H_j^k (k = 1, 2, \dots, d^N - 1)$ which are not contained in $Z(\mathbf{P})$, so that no two such elements are in the same $Z(\mathbf{P})$ -coset.
- Step 3 Then $\mathcal{U}(\mathcal{S}) := \{H_\alpha^\beta | \alpha \in \{0, 1, \dots, M\}, \beta \in \{1, 2, \dots, d^N - 1\}\}$ is a set of commuting unitary classes.
- Step 4 If \mathcal{S} is a *complete* partial spread of $\mathcal{W}_{2N-1}(d)$, that is, if \mathcal{S} is not strictly contained in *another* partial spread, then $\mathcal{U}(\mathcal{S})$ is unextendible, and the corresponding set of MUBs is weakly unextendible of size $M+1$.

In particular, this construction applies when $\mathcal{U}(\mathcal{S})$ is a set of Pauli operators (each $Z(\mathbf{P})$ -coset contains precisely one Pauli operator).

5.1. The bijection ρ . Let $\mathcal{G}(\mathcal{W}_{2N-1}(d))$ be the set of generators of $\mathcal{W}_{2N-1}(d)$, and let $\mathcal{C}(\mathbb{C}^{d^N})$ be the set of commuting classes of Pauli operators (of size $d^N - 1$). Note that from the above, it follows that we have a *bijection*

$$(1) \quad \rho : \mathcal{C}(\mathbb{C}^{d^N}) \longrightarrow \mathcal{G}(\mathcal{W}_{2N-1}(d))$$

which sends an element $\mathcal{U} \in \mathcal{C}(\mathbb{C}^{d^N})$ to a generator, following the scheme explained above. It is indeed a bijection: to each generator corresponds a unique maximal abelian subgroup $A \leq \mathbf{P} \leq \mathbf{U}_{d^N}(\mathbb{C})$ as above (and conversely), and each $Z(\mathbf{P})$ -coset in this subgroup contains precisely one Pauli operator. Together, the set of (nontrivial) Pauli operators in A form one commuting class of Pauli operators of size $d^N - 1$, that is, one element of $\mathcal{C}(\mathbb{C}^{d^N})$.

5.2. Prime dimension. Now let $N = 1$ (i.e., prime dimension) and $d \neq 2$. Then Proposition 4.2 tells us that \mathbf{P} is a group of size d^3 and exponent d , and its center has size d — in other words, \mathbf{P} is *extra-special*. In \mathbf{P} one can now choose subgroups H_j^i as above, and again [1] applies. If $d = 2$, the result is well known (but it can also be derived as above).

6. THE CASE d PRIME, $N = 2$ — SMALL AND LARGE EXAMPLES

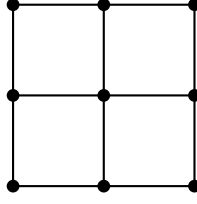
If $d = p$ is a prime and $N = 2$, the corresponding symplectic polar space is $\mathcal{W}_3(p) =: \mathcal{X}$, with ambient projective space $\mathbf{PG}(3, p)$, and it has two types of linear subspaces which are completely contained in \mathcal{X} , namely points of $\mathbf{PG}(3, p)$, and (projective) lines.

6.1. Grids and point-line duals. Before proceeding, we explore some synthetic properties of $\mathcal{W}_3(p)$ which will makes things easy below.

Let \mathcal{P} be the point set of $\mathcal{W} := \mathcal{W}_3(p)$, \mathcal{L} its line set, and let \mathbf{I} be the (symmetric) “incidence relation” on $(\mathcal{P} \times \mathcal{B}) \cup (\mathcal{B} \cup \mathcal{P})$ which says that $x \mathbf{I} L$ ($L \mathbf{I} x$) if and only if the point x is on the line L . Then this point-line geometry is a *generalized quadrangle* [13], and a very deep and extensive theory exists on these structures. Note that each line contains $p+1$ points and that on each point there are $p+1$ lines. Also, recall the following defining projection property for generalized quadrangles: if x is a point and X a line not containing x , there is a unique line $Y \mathbf{I} x$ which meets X (and then in a unique point).

Now consider the point-line geometry \mathcal{Q} with line set \mathcal{B} , point set \mathcal{P} and the same incidence relation \mathbf{I} — the so-called *point-line dual* of $\mathcal{W}_3(p)$. Then by [13, 3.2.1], \mathcal{Q} is isomorphic to the point-line geometry of an orthogonal quadric $\mathcal{Q}(4, p)$ in $\mathbf{PG}(4, p)$. Moreover, if $p = 2$, \mathcal{Q} and \mathcal{W} are isomorphic [13, 3.2.1].

Let “ \perp ” denote the orthogonality relation in $\mathcal{W}_3(p)$, and let V, W be arbitrary lines which do not meet. Then $\{V, W\}^\perp$ consists of $p+1$ lines which are mutually disjoint. If p is odd, $(\{V, W\}^\perp)^\perp$, the set of lines which meet all lines of $\{V, W\}^\perp$, is $\{V, W\}$. If $p = 2$, there is a third line X besides V, W in this set.

FIGURE 1. A (3×3) -grid.

The set of points on the lines of $\mathcal{R}_1 := \{V, W\}^\perp$, which is the same as the set of points on the lines of $\mathcal{R}_2 := (\{V, W\}^\perp)^\perp$, forms a (3×3) -grid \mathcal{G} , and the aforementioned line sets $\mathcal{R}_1, \mathcal{R}_2$ are the reguli of this grid.

Also, an easy counting exercise shows that all lines of $\mathcal{W}_3(2)$ have at least one point in common with the point set of $V \cup W \cup X$. (All these properties can essentially be found in [13, Chapter 3].)

6.2. Antiregularity. If ℓ is any odd prime power, we will use the fact that $\mathcal{W}_3(\ell)$ has no (3×3) -grids. This is a corollary of a property called “antiregularity,” and can be found in [13, 3.3.1(i), dual].

6.3. The case $p = 2$. We start with giving an alternative and very short proof of Theorem 1 of [10] using the connection between Pauli classes and partial spreads of symplectic polar spaces.

Theorem 6.1 (Mandayam et al. [10]). *Given three Pauli classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ belonging to a complete set \mathcal{S} of classes in $d = 4$, there exists exactly one more maximal commuting class \mathcal{C} of Pauli operators in $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$. The class \mathcal{C} together with the remaining two classes \mathcal{C}_4 and \mathcal{C}_5 of \mathcal{S} forms a unextendible set of Pauli classes, whose common eigenbases form a weakly UMUB of order 3.*

Proof. Interpret \mathcal{S} in $\mathcal{W}_3(2)$; then by Theorem 5.1 to the \mathcal{C}_i correspond lines L_i of $\mathcal{W}_3(2)$ ($i = 1, \dots, 5$), and they form a spread. Consider the lines L_1, L_2, L_3 . Then either there is precisely one line L of $\mathcal{W}_3(2)$ meeting them all, or there are three such lines. In the latter case the lines L_1, L_2, L_3 form a regulus of a (3×3) -grid, and as we have seen any line of $\mathcal{W}_3(2)$ meets the point set of such a grid, leading to the fact that L_1, L_2, L_3 would not be extendible to a spread, contradiction. So we are in the former case, and the class \mathcal{C} corresponding to L is the one of the statement. The set $\mathcal{C}, \mathcal{C}_4, \mathcal{C}_5$ obviously is unextendible, since extending it with a class $\tilde{\mathcal{C}}$ would mean that the corresponding line \tilde{L} be contained in the point set of $L_1 \cup L_2 \cup L_3$, implying that there would be another line besides L meeting all of L_1, L_2, L_3 , contradiction. ■

We now give a short proof of another result of [10], namely Theorem 5 of that paper.

Theorem 6.2 (Mandayam et al. [10]). *Given an unextendible set of three Pauli classes $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ in $d = 4$, the nine operators in $\mathcal{C}_1 \cup \mathcal{C}_2 \cup \mathcal{C}_3$ can be partitioned into a different set of three maximal commuting classes $\mathcal{C}'_1, \mathcal{C}'_2, \mathcal{C}'_3$ such that each \mathcal{C}'_i has precisely one operator in common with each \mathcal{C}_j , $i, j \in \{1, 2, 3\}$.*

Proof. Let L_1, L_2, L_3 the lines corresponding to $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3$ in $\mathcal{W}_3(2)$; we have seen that either one or three lines are contained in $\{L_1, L_2, L_3\}^\perp$; in the latter case, an easy counting argument shows that all lines of $\mathcal{W}_3(2)$ intersect with $L_1 \cup L_2 \cup L_3$, so suppose we are in the former case, and let $\{L\} := \{L_1, L_2, L_3\}^\perp$. Then each point on L is incident with precisely one line besides L and not in $\{L_1, L_2, L_3\}$. By the projection property of generalized quadrangles, there are six lines different from L_1, L_2, L_3 which meet the six points of $L_1 \cup L_2 \cup L_3$ not on L in precisely two points. So the total number of lines meeting $L_1 \cup L_2 \cup L_3$ is 13, and $\{L_1, L_2, L_3\}$ is indeed extendible (since there are 15 lines in total). ■

In the next subsection, we will see a general approach for constructing unextendible Pauli classes in \mathbb{C}^{d^2} with d a prime number, starting from a complete set. As a corollary, we will obtain yet another proof for the result of Mandayam et al.

6.4. General case.

Theorem 6.3 (Existence of unextendible Pauli class sets for d prime, A). *For each prime $d = p$ there exists an unextendible set of Pauli classes \mathcal{S} of size $d^2 - d + 1$ or $d^2 - d + 2$ in \mathbb{C}^{d^2} . The common eigenbases form a weakly UMUB of order $d^2 - d + 1$ or $d^2 - d + 2$.*

Proof. As before, we pass to $\mathcal{W}_3(p)$. Let \mathcal{T} be any spread of $\mathcal{W}_3(p)$.

Now let U be any line of $\mathcal{W}_3(p)$ which is not contained in \mathcal{T} ; then there are precisely $p + 1$ lines in \mathcal{T} which hit U (each in exactly one point), due to the fact that the lines of \mathcal{T} partition the point set of $\mathcal{W}_3(p)$. Call this line set \mathcal{T}_U . Now consider the line set

$$(2) \quad \mathcal{T}(U) := \mathcal{T} \setminus \mathcal{T}_U \cup \{U\}.$$

Note that $|\mathcal{T}(U)| = p^2 - p + 1$. If it is not a complete partial spread, there is at least one other line R of $\mathcal{W}_3(p)$ not meeting any line of $\mathcal{T}(U)$, and as a point set it clearly must be contained in the point set “of” \mathcal{T}_U . And then all lines of \mathcal{T}_U meet both U and R . If yet another line R' would exist that extends $\mathcal{T}_U \cup \{R\}$, R' would also be met by the lines of \mathcal{T}_U — in other words, $R' \in \mathcal{T}_U^\perp$ while $\mathcal{T}_U = U^\perp \cap R^\perp$. As we have seen, this is not possible, so only at most one line R can be added.

Translating back to Pauli classes gives the desired result. ■

It is easy to see that both cases of Theorem 6.7 can occur.

As we have not used the fact that p is prime, we can translate immediately to symplectic polar spaces over any finite field.

Corollary 6.4. *For each prime power ℓ there exists a complete partial spread \mathcal{S} of $\mathcal{W}_3(\ell)$ of size $\ell^2 - \ell + 1$ or $\ell^2 - \ell + 2$.* ■

Remark 6.5. For ℓ even, we have seen this result in the literature (see, e.g. [3] and the references therein) — it would be safe to attribute this result to folklore though. We presume the odd case is somewhere as well, but the way of proving is needed below, so it is included anyhow for the sake of completeness.

One could apply the technique in the proof of Theorem 6.7 multiple times to obtain examples with less elements. And indeed, this works quite well, as we will demonstrate now. We will work immediately in $\mathcal{W}_3(\ell)$, and will not restrict ourselves only to the prime case. So ℓ is a prime power. We do ask that ℓ is odd — it will be used in the proof.

Let \mathcal{S} be a *classical spread* of $\mathcal{W}_3(\ell)$ — by this, we mean a spread which in the point-line dual $\mathcal{Q}(4, \ell)$ corresponds to an elliptic quadric. Take any two lines L, M in \mathcal{S} , and consider the set $\mathcal{X} = \{X_0, X_1, \dots, X_\ell\} := \{L, M\}^\perp$; it consists of $\ell + 1$ mutually disjoint lines which are not in \mathcal{S} . Now for each $X_i \in \mathcal{X}$, define \mathcal{S}_i to be the set of $\ell + 1$ lines of \mathcal{S} meeting X_i . As explained in Appendix B of this paper, for each \mathcal{S}_i there is precisely one more line $\widetilde{X}_i \neq X_i$ which meets each line of \mathcal{S}_i . Clearly, this line must be in \mathcal{X} , so we can denote \widetilde{X}_i by $X_{\widetilde{i}}$.

Now the following properties are immediate:

- (a) $(\cdot)^\sim : \{0, 1, \dots, \ell\} \longrightarrow \{0, 1, \dots, \ell\}$ is an involution, so that $|\{\mathcal{S}_0, \mathcal{S}_1, \dots, \mathcal{S}_\ell\}| = (\ell + 1)/2$;
- (b) for $\mathcal{S}_i \neq \mathcal{S}_j$, we have that $\mathcal{S}_i \cap \mathcal{S}_j = \{L, M\}$.

For the sake of convenience, we re-write the set $\{\mathcal{S}_0, \mathcal{S}_1, \dots, \mathcal{S}_\ell\}$ as $\{\mathcal{S}_0, \mathcal{S}_1, \dots, \mathcal{S}_{(\ell-1)/2}\}$. For each $j \in \{0, 1, \dots, (\ell-1)/2\}$ we have that $\{X_j, X_{\widetilde{j}}\}^\perp = \mathcal{S}_j$.

Theorem 6.6. *Let ℓ be an odd prime power. Then for any $k = 0, 1, \dots, (\ell-3)/2$, there exist complete partial spreads of size $\ell^2 - (k+1)\ell + (3k+1)$ in $\mathcal{W}_3(\ell)$.*

Proof. Let k be as in the statement, and consider any subset R of $\{0, 1, \dots, (\ell - 1)/2\}$ of size $k + 1$; for simplicity, we consider w.l.o.g. the set $\{0, 1, \dots, k\}$. Then define the following set:

$$(3) \quad \mathcal{S}_R := \mathcal{S} \setminus (\cup_{u \in R} \mathcal{S}_u) \cup_{v \in R} (\{X_v, X_{\bar{v}}\}).$$

It is straightforward to see that \mathcal{S}_R is a partial spread of size $\ell^2 - (k + 1)\ell + (3k + 1)$. As for completeness, suppose we could enlarge \mathcal{S}_R with some line U to another partial spread. As \mathcal{S} is a spread, U must be contained in $\cup_{u \in R} \mathcal{S}_u$, and it cannot be contained in \mathcal{S} nor \mathcal{S}_R . By the Pigeon Hole Principle, some \mathcal{S}_w must have at least three lines meeting U since U has $d + 1$ points and $k + 1 < \frac{d+1}{2}$ (in case $U \in \{L, M\}^\perp$, one does not need the Pigeon Hole Principle). However, this implies the existence of a (3×3) -grid, contradiction. ■

For each odd prime power ℓ the bounds appear to be new (up to some small coincidences). For fixed ℓ , we obtain complete partial spreads of respective sizes

$$(4) \quad \ell^2 - \ell + 1, \ell^2 - 2\ell + 4, \ell^2 - 3\ell + 7, \dots, \frac{\ell^2}{2} + 2\ell - \frac{7}{2}.$$

Translating back to Pauli operators, we obtain the next result.

Theorem 6.7 (Existence of unextendible Pauli class sets for d prime, B). *For each odd prime $d = p$ and any $k = 0, 1, \dots, (d - 3)/2$ there exists an unextendible set of Pauli classes \mathcal{S} of size $d^2 - (k + 1)d + (3k + 1)$ in \mathbb{C}^{d^2} . The common eigenbases form a weakly UMUB of order $d^2 - (k + 1)d + (3k + 1)$.* ■

The construction has many variations, all using roughly the same ideas, and all giving similar (but not the same) bounds. We will come back to these variations in a forthcoming paper.

7. SOLUTION OF CONJECTURE 1.2

Motivated by Theorem 1.1, the following conjecture is then stated in [10].

CONJECTURE 7.1 (Mandayam et al. [10]). *Given $\ell/2 + 1$ maximal commuting Pauli classes $\mathcal{C}_1, \mathcal{C}_2, \dots, \mathcal{C}_{\ell/2+1}$ belonging to a complete set \mathcal{S} of classes in $\ell = 2^N =: d^N$, $N \in \mathbb{N} \setminus \{0, 1\}$, there exists exactly one more maximal commuting class \mathcal{C} of Pauli operators in $\cup_{1 \leq i \leq \ell/2+1} \mathcal{C}_i$. The class \mathcal{C} together with the remaining classes of \mathcal{S} forms an unextendible set of Pauli classes of size $\ell/2 + 1$, whose common eigenbases form a weakly UMUB of order $\ell/2 + 1$.*

In this section we will show that this conjecture is true *if and only if* $N = 2$ or $N = 3$. In fact, we will consider the conjecture in any characteristic d (i.e., for any prime d), and show that it is true if and only if $d = 2$ and $N = 2$ or $N = 3$.

Translated to the geometric setting, we obtain: “given $2^{N-1} + 1$ elements $\alpha_1, \alpha_2, \dots, \alpha_{2^{N-1}+1}$ belonging to a spread \mathcal{S} of the polar space $\mathcal{W}_{2N-1}(2)$, there exists exactly one more generator χ which is completely contained in the union of these elements, such that χ together with the remaining elements of \mathcal{S} constitutes a complete partial spread.”

Note that the situation implies that χ meets each α_j , $j = 1, 2, \dots, 2^{N-1} + 1$.

We will replace $d = 2$ by any prime d , and consider the same situation (immediately in the geometric setting). We will also slightly generalize the statement by replacing “exactly one” by “at least one.”

So let \mathcal{S} be a spread of $\mathcal{W}_{2N-1}(d)$, d a prime. We assume that the conjecture above is true (in the more general setting).

First suppose that \mathcal{U} and \mathcal{U}' are different subsets of \mathcal{S} , both of size $d^{N-1} + 1$. Let α be a generator which meets all elements of \mathcal{U} and is covered by these elements, and let α' be a generator which meets all elements of \mathcal{U}' and is covered by them. Then $\alpha \neq \alpha'$.

In the next counting argument, we will use the fact that the number of generators of $\mathcal{W}_{2N-1}(d)$ is $(d^N + 1)(d^{N-1} + 1) \cdots (d + 1)$. Per subset of \mathcal{S} of size $d^{N-1} + 1$, by the conjecture we have at least one

generator meeting all of its elements, and covered by them. Such a generator is never contained in \mathcal{S} . So we have that

$$(5) \quad C_{|\mathcal{S}|}^{d^{N-1}+1} \cdot 1 + |\mathcal{S}| \leq (d^N + 1)(d^{N-1} + 1) \cdots (d + 1).$$

Here,

$$(6) \quad C_{|\mathcal{S}|}^{d^{N-1}+1} := \frac{(d^N + 1)!}{(d^{N-1} + 1)!(d^N - d^{N-1})!}.$$

(Note that equality should hold in (5) in the “precisely one statement.”)

Now (5) is equivalent to

$$(7) \quad \frac{(d^N + 1)d^N \cdots (d^N - d^{N-1} + 1) + (d^{N-1} + 1)!(d^N + 1)}{(d^{N-1} + 1)!(d^N + 1)(d^{N-1} + 1) \cdots (d + 1)} \leq 1,$$

or, slightly simplified:

$$(8) \quad \frac{((d^N + 1)/(d^{N-1} + 1))(d^N/d^{N-1}) \cdots ((d^N - d^{N-1} + 1)/(1)) + (d^N + 1)}{(d^N + 1)(d^{N-1} + 1) \cdots (d + 1)} \leq 1.$$

Now note that

$$(9) \quad ((d^N + 1)/(d^{N-1} + 1))(d^N/d^{N-1}) \cdots ((d^N - d^{N-1} + 1)/(1)) \geq \frac{d^N + 1}{d^{N-1} + 1} \cdot d^{d^{N-1}},$$

and that

$$(10) \quad (d^N + 1)(d^{N-1} + 1) \cdots (d + 1) \leq d^{N+1}d^N \cdots d^2 = d^{N(N+3)/2}.$$

Observe that if for some value $N = M$, we have

$$(11) \quad d^{d^{M-1}} \geq d^{M(M+3)/2},$$

then the same inequality holds for all $M' \geq M$.

This is already enough to conclude with a contradiction for $d \geq 5$; $d = 3$ and $N \geq 3$; and $d = 2$ and $N \geq 6$. The cases $(d, N) = (3, 2), (2, 5), (2, 4)$ all yield a contradiction when substituted in (5); the substitution $(d, N) = (2, 2)$, which is precisely the case of $\mathcal{W}_3(2)$ which was already studied before, leads to equality in (5), as does the substitution $(d, N) = (2, 3)$, which is the case of $\mathcal{W}_5(2)$. ■

Note that the cases $(d, N) = (2, 2), (2, 3)$ are precisely those handled in §3, Theorem 1 and §3, Theorem 3 of [10].

In the next section we will formulate and discuss variations on Conjecture 1.2; to that end, we first try to generalize Theorem 6.7.

8. EXISTENCE OF MAXIMAL PAULI CLASSES

Before proceeding, let us first introduce a simple lemma about complete “partial spreads” of general incidence structures. Let $\Gamma = (\mathcal{E}, t, T)$ be a triple, with $T = \{0, 1, \dots, n\}$, $n \in \mathbb{N}^\times$, and t a surjective function from the set $\mathcal{E} \neq \emptyset$ to T . For each $i \in \{0, 1, \dots, n\}$, put $\mathcal{E}_i := t^{-1}(i)$, and call its elements the elements of type i . So

$$(12) \quad \mathcal{E} = \cup_{i \in T} \mathcal{E}_i, \text{ and } |\mathcal{E}| \geq |T|.$$

In particular, we call elements of \mathcal{E}_0 “points.” We now assume that for $i > 0$, every element of \mathcal{E}_i is a subset of \mathcal{E}_0 . This is a natural assumption: we see each “ i -space” (= element of type i) as a point set.

An i -spread of Γ is a partition of \mathcal{E}_0 in elements of type i . Complete i -spreads are introduced naturally as above.

Proposition 8.1. *Let \mathcal{S} be an i -spread of Γ . Let χ be an element of type i which is not contained in \mathcal{S} , and let \mathcal{S}_χ be the subset of elements of \mathcal{S} which meet χ in at least one point. Note that \mathcal{S}_χ induces a partition of the points of χ . Then if we cannot find a set \mathcal{T} of elements of type i such that*

C.1 *each element of \mathcal{T} is a subset of the point set*

$$(13) \quad \Omega(\mathcal{S}, \chi) := \cup_{U \in \mathcal{S}_\chi} U;$$

C.2 *the elements of \mathcal{T} partition $\Omega(\mathcal{S}, \chi)$,*

we have that $\mathcal{S} \setminus \mathcal{S}_\chi \cup \{\chi\}$ cannot be completed to an i -spread of Γ .

Proof. If $\mathcal{S} \setminus \mathcal{S}_\chi \cup \{\chi\}$ could be completed to an i -spread \mathcal{S}' of Γ , \mathcal{S}' must have elements which all are subsets of $\Omega(\mathcal{S}, \chi)$, and which partition Γ . ■

If ℓ is the maximum number of elements of type i contained in Ω as subsets and which are two by two disjoint, the number of elements in a maximal partial i -spread containing $\mathcal{S} \setminus \mathcal{S}_\chi \cup \{\chi\}$ is at most $|\mathcal{S}| - |\mathcal{S}_\chi| + \ell$. (Note that $\ell \geq 1$ as χ itself is in $\Omega(\mathcal{S}, \chi)$.)

Remark 8.2 (Back to the prime case). Note that the first part of Theorem 6.7 is an application of the construction method of Proposition 8.1 (with $\chi = L$).

8.1. \mathcal{U} -Sets. Motivated by Proposition 8.1, a \mathcal{U} -set with carrier χ is a set \mathcal{S}_χ of mutually disjoint generators of $\mathcal{W}_{2N-1}(d)$ which all meet some generator $\chi \notin \mathcal{S}_\chi$ such that

$$(14) \quad \chi \subset \cup_{Y \in \mathcal{S}_\chi} Y,$$

and such that $\cup_{Y \in \mathcal{S}_\chi} Y$ cannot be partitioned by a partial spread \mathcal{P} of generators which includes χ .

Note that the number of elements of an \mathcal{U} -sets is not uniquely determined by N and d . (One \mathcal{U} -set could also have different carriers.)

Proposition 8.3 (Existence of UMUBs, I). *The existence of \mathcal{U} -sets implies the existence of complete partial spreads which are not spreads, that is, of unextendible sets of Pauli classes.*

Proof. Let \mathcal{S}_χ be a \mathcal{U} -set. If \mathcal{S}_χ is not contained in a spread, then we are done, so suppose it is contained in some spread \mathcal{S} . Then by Proposition 8.1 we have that $\mathcal{S} \setminus \mathcal{S}_\chi \cup \{\chi\}$ cannot be completed to a spread. ■

Note that this proposition can also be applied to general incidence geometries.

For the rest of this section, we suppose d is an odd prime.

Before proceeding, recall that a spread \mathcal{S} (of generators) of $\mathcal{W}_{2N-1}(d)$ is *regular* if the following property is satisfied: if for every three distinct elements α, β, γ in \mathcal{S} , \mathcal{L} is the set of lines of $\mathbf{PG}(2N-1, d)$ which meet each of α, β, γ , then there are $d-2$ further elements of \mathcal{S} which meet every line in \mathcal{L} . It is well known that every symplectic polar space has regular spreads.

Now let \mathcal{R} be a regular spread of $\mathcal{W}_{2N-1}(d)$. Take a generator χ which meets some $\alpha \in \mathcal{R}$ in a space of dimension $N-2$ (and note that this is possible), and let \mathcal{R}_χ be the set of elements in \mathcal{R} which meet χ . Note that $|\mathcal{R}_\chi| = d^{N-2} + 1$. Now consider a generator $\beta \neq \chi, \alpha$ which contains $\chi \cap \alpha$, and which is disjoint from the elements in $\mathcal{R}_\chi \setminus \{\alpha\}$. (For the existence of such a generator, see Appendix A.) Then because \mathcal{R} is a regular spread, one notes that $\mathcal{S}_\chi := \mathcal{R}_\chi \setminus \{\alpha\} \cup \{\beta\}$ is a \mathcal{U} -set. For, suppose that $\cup_{Y \in \mathcal{S}_\chi} Y$ can be partitioned by a partial spread \mathcal{P} of generators which includes χ . Let $\gamma \in \mathcal{P} \setminus \{\chi\}$ contain some point b of β ; then $\gamma \cap \beta = \{b\}$. Let B be any line in γ containing b ; then B meets $d+1$ different elements of \mathcal{S}_χ , one of which is β . As $d \geq 3$, the fact that \mathcal{R} is a regular spread implies that $b \in \alpha$, contradiction.

In the next theorem, we prove that unextendible sets of Pauli classes of \mathbb{C}^{d^N} always exist (ignoring possible sizes completely), that is, that complete partial spreads which are not spreads always exist in $\mathcal{W}_{2N-1}(d)$. This fact is not necessarily true for general incidence geometries which have i -spreads (using

the nomenclature of above): consider for instance an incidence geometry for which the elements of type i precisely form *one* i -spread. So although the existence of complete partial spreads is probably seen as folklore, we see the need to formally write it down.

Theorem 8.4 (Existence of UMUBs, II). *Every Hilbert space \mathbb{C}^{d^N} , with d an odd prime and N a positive integer, contains weakly unextendible sets of Pauli classes.*

Proof. Translated to $\mathcal{W}_{2N-1}(d)$, we need to show that the latter geometry always contains complete partial spreads which are not spreads. So take a regular spread \mathcal{R} . Consider a generator χ as above, and construct the \mathcal{U} -set $\mathcal{S}_\chi := \mathcal{R}_\chi \setminus \{\alpha\} \cup \{\beta\}$. Now apply Proposition 8.3. ■

Remark 8.5. Note that if \mathcal{R}_χ in the proof of the previous theorem is such that there does not exist a generator besides χ which is contained in $\cup_{\alpha \in \mathcal{R}_\chi} \alpha$, then

$$(15) \quad |\mathcal{R} \setminus \mathcal{R}_\chi \cup \{\chi\}| = d^N - d^{N-1} + 1.$$

In the special case $d = 2$, we would end up with an unextendible set of Pauli classes of size $2^{N-1} + 1$.

8.2. Reformulation of Conjecture 7.1. We have seen that Conjecture 7.1 is only true when $N = 2$ or $N = 3$. On the other hand, there seems to be some evidence that the bound of that conjecture could be attained (see, e.g., the previous remark). So we reformulate the conjecture as follows — we will do it in geometric terms, over all fields \mathbb{F}_ℓ with ℓ a prime power, but again, for the applications in Quantum Information Theory, one takes ℓ to be prime.

Corollary 8.6. *For each prime power ℓ and positive integer $N \geq 2$, there exists a spread \mathcal{S} of $\mathcal{W}_{2N-1}(\ell)$ and a generator χ not in \mathcal{S} , such that $\mathcal{S} \setminus \mathcal{S}_\chi \cup \{\chi\}$ is a complete partial spread of size $d^N - d^{N-1} + 1$.*

When $d = 2$, one obtains the same bound as in Conjecture 7.1.

We hope to come back to this conjecture in the near future.

9. “GALOIS MUBS”

When $d = 2, 3, 5, 7$ or 11 , there exist extremely exotic examples of unextendible sets of Pauli classes of size $d^2 - 1$ in \mathbb{C}^{d^2} . (Details, constructions and references can be found in [4].) We propose to call the corresponding sets of MUBs “Galois MUBs,” because they are all related to exotic 2-transitive representations of special linear groups, as was first noted by Galois (see also [4]). They are extremely special amongst Pauli classes of \mathbb{C}^{d^2} , d a prime, or even *all* Hilbert spaces, due to the following result.

Theorem 9.1 (See [13], §2.7). *Let Γ be a generalized quadrangle of finite thick order (s, s) , and let \mathcal{C} be a complete partial spread of Γ . If Γ is not contained in a spread of Γ , then*

$$(16) \quad |\mathcal{C}| \leq s^2 - 1.$$

As we have seen that the points and lines of any $\mathcal{W}_3(d)$ form a generalized quadrangle, this result applies to $\mathcal{W}_3(d)$ and hence also to Pauli classes in \mathbb{C}^{d^2} .

Corollary 9.2. *A set of commuting Pauli classes of size d^2 in \mathbb{C}^{d^2} , d a prime, is never unextendible.* ■

Remark 9.3. The aforementioned examples in $d = 2, 3, 5, 7, 11$ are the only known examples which effectively reach the $(d^2 - 1)$ -bound, and conjecturally they are the only ones. Geometrically, they also satisfy very extreme properties, which rightly translate to Pauli classes. Much more details on the geometric structure of partial spreads of size $s^2 - 1$ in generalized quadrangles of order (s, s) can be found in the author’s paper [18].

The next theorem, taken from the author’s paper [18], says that when $d = 2$, up to isomorphism there is only one complete partial spread of size $3 = 2^2 - 1$ in $\mathcal{W}_3(2)$.

Theorem 9.4 ([18]). *Up to isomorphism there is only one complete partial spread of size 3 in $\mathcal{W}_3(2)$.*

Corollary 9.5. *Up to isomorphism, there is only one unextendible set of Pauli classes of size 3 in \mathbb{C}^4 .* ■

Remark 9.6 (On isomorphisms). Of course, one needs to specify *what* isomorphisms between unextendible sets of Pauli classes *are*. Because of the General Connecting Theorem (and the bijection ρ), we propose to say that unextendible sets of Pauli classes \mathcal{U} and \mathcal{U}' in \mathbb{C}^{d^N} are *isomorphic* if there exists an automorphism of $\mathcal{W}_{2N-1}(d)$ which maps the complete partial spread $\mathcal{S}(\mathcal{U})$ corresponding to \mathcal{U} , to the complete partial spread $\mathcal{S}(\mathcal{U}')$ corresponding to \mathcal{U}' . This is a natural notion of “isomorphism,” since automorphisms of $\mathcal{W}_{2N-1}(d)$ preserve collinearity of points, so also the commuting of operators at the level of Pauli operators. (One could also define isomorphisms through the general Pauli group. On the other hand, such automorphisms induce automorphisms of $\mathcal{W}_{2N-1}(d)$ anyhow, while the converse is *not* true. So one misses (many) maps which should be considered as isomorphisms in this way.)

10. CONCLUSION

The geometry underlying the space of the generalized Pauli operators/matrices characterizing N d -level quantum systems, with $N \geq 2$ and d any prime, is that of the symplectic polar space of rank N and order d , $\mathcal{W}_{2N-1}(d)$.

Using this connection, we have derived a short proof of a recent result of [10] on the unextendibility of MUB sets in \mathbb{C}^4 (their Theorem 1). Moreover, we generalized this result for all $d = \text{square of a prime}$, and presented a construction of a class of maximal partial spreads of $\mathcal{W}_3(\ell)$ for any odd prime power ℓ , attaining new bounds in generically every case, which rightly translates to UMUBs in the case ℓ is a prime. We also gave a very short proof of Theorem 5 of [10].

We then considered Conjecture 1 of [10] which conjecturally generalizes the aforementioned result of [10] to *any* dimension and showed that it is true *if and only if* $N = 2$ or $N = 3$.

We then indicated that an alternative version of the conjecture might be true, and described several new construction techniques to obtain weakly unextendible sets of MUBs.

Finally, we discussed a special kind of weakly unextendible sets of MUBs, called “Galois MUBs,” which attain an optimal bound in relation to being unextendible.

APPENDIX A. PROPERTIES OF (SYMPLECTIC) POLAR SPACES

Consider the space $\mathcal{W}_{2N-1}(d)$, d a prime, $N \geq 2$. (We restrict ourselves to the prime case because that's the class which translates to Pauli operators, but everything works when d is a prime power as well.)

A.1. Let γ be a generator, and x a point not in γ . Then a well-known property (of general polar spaces) — see e.g. [20, p.137, (c)] — says that there is a unique generator on x which meets γ in an $(N-2)$ -space, $\gamma(x)$. (If “ \perp ” is the orthogonality relation coming from the associated alternating form, then $\gamma(x) = x^\perp \cap \gamma$.) Now let γ and γ' be disjoint generators. Then it is not hard to see that for every $(N-2)$ -space δ in γ' , there is precisely one point $y \in \gamma$ such that $\langle y, \delta \rangle$ is a generator ($y = \gamma \cap \delta^\perp$). So the map

$$(17) \quad \mu : \gamma \longrightarrow \gamma' : x \longrightarrow \gamma'(x)$$

is a bijection between the points of γ and the hyperplanes of γ' .

A.2. Now let α be an $(N-2)$ -space contained in $\mathcal{W}_{2N-1}(d)$; it is well-known that there are $d+1$ generators g_0, \dots, g_d containing α . Let β be a generator disjoint from α . By the surjectivity above, it follows that some g_i has to intersect β , and then necessarily in one point.

A.3. **Structure of spreads.** Let \mathcal{S} be a spread of $\mathcal{W}_{2N-1}(d)$, d a prime, $N \geq 2$. Let $\alpha = g_0 \in \mathcal{S}$, and let τ be an $(N-2)$ -space in α . Let g_1, \dots, g_d be the other generators containing τ . By the previous paragraph, each element of $\mathcal{S} \setminus \{\alpha\}$ meets some g_i ($i \neq 0$) in precisely one point. And conversely, each point of $g_j \setminus \tau$ is contained in precisely one spread element. Indeed,

$$(18) \quad (|\mathcal{S}| - 1) \cdot 1 = d^N = d \cdot d^{N-1} = \sum_{i=1}^d \#(\text{points of } g_i \setminus \tau).$$

APPENDIX B. SOME MORE PROPERTIES OF $\mathcal{W}_3(d)$

As in the first appendix, for the applications in Quantum Information Theory considered here, one wants to think of d as being prime, but everything holds when d is a prime power as well. What we *do* ask is that d is odd.

Let \mathcal{S} be a classical spread of $\mathcal{W}_3(d)$; point-line dualize to obtain $\mathcal{Q}(4, d)$ — \mathcal{S} becomes an elliptic quadric, denoted \mathcal{O} . Now let x be a point of $\mathcal{Q}(4, d)$ not contained in \mathcal{O} . As usual, let “ \perp ” denote the orthogonality relation associated to the defining quadratic form of $\mathcal{Q}(4, d)$ (say, corresponding to the variety with equation $X_0^2 + X_1X_2 + X_3X_4 = 0$). Then $x^\perp \cap \mathcal{O}$ is a conic section, and since d is odd, there is precisely one other point $y \notin \mathcal{O}$ for which

$$(19) \quad y^\perp \cap \mathcal{O} = x^\perp \cap \mathcal{O}.$$

Note that the latter expression is equal to $\{x, y\}^\perp$.

Going back to $\mathcal{W}_3(d)$ (i.e., dualizing again), we obtain that if X is a line of $\mathcal{W}_3(d)$ not in \mathcal{S} , and \mathcal{S}_X is the set of $d + 1$ lines in \mathcal{S} which meet X , then there is precisely one other line Y not in \mathcal{S} such that

$$(20) \quad \mathcal{S}_X = \{X, Y\}^\perp = X^\perp \cap Y^\perp = \mathcal{S}_Y.$$

REFERENCES

- [1] Bandyopadhyay A, Boykin, P O, Roychowdhury V and Vatan F 2002 *Algorithmica* **34** 512–528
- [2] Bengtsson I 2005 AIP Conference Proceedings **750** 63–69 (*Preprint* quant-ph/0406174)
- [3] Cimrakova M, De Winter S, Fack V and Storme L 2007 *European J Combin* **28** 1934–1942
- [4] De Winter S and Thas K 2010 *Innov. Incidence Geom.* **11** 19–33
- [5] Havlicek H and Saniga M 2007 *J. Phys. A* **40**, F943–F952
- [6] Havlicek H and Saniga M 2008 *J. Phys. A* **41** Article ID 015302
- [7] Hirschfeld J W P 1998 *Projective Geometries over Finite Fields (2nd Edition)* Oxford Mathematical Monographs (New York: Oxford University Press)
- [8] Klappenecker A and Roetteler M 2005 Proc. 2005 IEEE International Symposium on Information Theory 1740–1744 (*Preprint* quant-ph/0502031)
- [9] Lawrence J, Brukner C and Zeilinger A 2002 *Phys. Rev. A* **65** 032320
- [10] Mandayam, Bandyopadhyay A, Grassl and Wootters W K 2014 *Quantum Inf. Comp* **14** 0823–0844
- [11] David Mermin N 1990 *Phys. Rev. Lett.* **65** 3373–3376
- [12] Mosseri R and Dandoloff R 2001 *J. Phys. A.: Math. Gen.* **34** 10243–10252
- [13] Payne, S E and Thas J A 1984 *Finite Generalized Quadrangles* Research Notes in Mathematics **110** (Pitman (Advanced Publishing Program): Boston, MA)
- [14] Saniga M and Planat M 2006 *J. Phys. A.: Math. Gen.* **39** 435–440 (*Preprint* math-ph/0506057)
- [15] Saniga M, Planat M and Pracna P 2008 *Theoretical and Mathematical Physics* **155** 905–913 (*Preprint* quant-ph/0611063)
- [16] Saniga M and Planat M 2007 *Advanced Studies in Theoretical Physics* **1** 1–4 (*Preprint* quant-ph/0612179)
- [17] Thas J A 2001 Ovoids, spreads and m -systems of finite classical polar spaces *London Math. Soc. Lecture Note Series* **288** (Cambridge: Cambridge University Press) pp 241–267
- [18] Thas K 2002 *J. Combin. Theory Ser. A* **97** 394–402
- [19] Thas K 2009 *Europhys. Lett. (EPL)* **86** 60005
- [20] Ueberberg J 2011 *Foundations of Incidence Geometry. Projective and polar spaces* Springer Monographs in Math. (Springer: Heidelberg)
- [21] Wootters W K and Fields B D 1989 *Ann. Phys.* **191** 363–381
- [22] Wootters W K 2004 *IBM J. Res. Dev.* **48** 99–110
- [23] Wootters W K 2006 *Found. Phys.* **36** 112–126

DEPARTMENT OF MATHEMATICS, GHENT UNIVERSITY, KRIJGSLAAN 281, S25, B-9000 GHENT, BELGIUM
E-mail address: koen.thas@gmail.com